

General AI Technology Audit - Pre-Deployment

Focus Area: Enterprise Decision Engines, Predictive AI Systems, & LLM Integrations

Framework Alignment: NIST AI RMF 1.0, ISO/IEC 42001, EU AI Act

1. Governance & Classification

Control ID	Audit Requirement / Question	Regulatory Trigger
GEN-PRE-01	Is a formal AI Risk Tier Classification (Unacceptable, High, Medium, Low) documented for the use case?	EU AI Act Risk Tiers / ISO 42001
GEN-PRE-02	Has a certified Model Card been delivered detailing training data provenance, baseline limits, and edge-case failures?	NIST AI RMF Govern
GEN-PRE-03	Is a Human-in-the-Loop (HITL) approval boundary defined for automated outputs exceeding designated financial or operational impact thresholds?	ISO/IEC 42001 Standard
GEN-PRE-04	Is an operational rollback/kill-switch procedure documented to immediately isolate the model if unpredicted behavior occurs?	Enterprise Risk Control

2. Robustness, Security & Red-Teaming

Control ID	Audit Requirement / Question	Regulatory Trigger
GEN-PRE-05	Has the model undergone red-teaming against prompt injection, jailbreaking, and training data extraction exploits?	OWASP Top 10 for LLMs
GEN-PRE-06	Are hallucination rates, toxicity levels, and accuracy benchmarks quantified against domain-specific test sets?	NIST AI RMF Measure
GEN-PRE-07	Has the training/RAG pipeline been audited to ensure no unauthorized Proprietary Information or PII was ingested without consent?	GDPR / CCPA / IP Law

3. Explainability & User Transparency

Control ID	Audit Requirement / Question	Regulatory Trigger
GEN-PRE-08	Can the model produce global feature importance (SHAP) or localized decision rationale (LIME) for automated decisions?	EU AI Act Transparency Mandates
GEN-PRE-09	Is clear system disclosure provided informing end-users that they are interacting with or being evaluated by an AI system?	FTC Guidance / EU AI Act Art. 50